JOURNAL OF NUMBER THEORY **60**, 254–290 (1996)
ARTICLE NO. 0123

Fermat–Euler Theorem in Algebraic Number Fields

Miroslav Laššák*

Institute of Mathematics, Slovak Academy of Sciences, Štefánikova 49, 814 73 Bratislava, Slovak Republic

and

Štefan Porubský†

Department of Mathematics, Prague Institute of Chemical Technology, Technická 1905, 166 28 Prague 6, Czech Republic

Communicated by Alan C. Woods

In this paper a (maximal) generalization of the classical Fermat–Euler theorem for finite commutative rings with identity is proved. Maximal means that we show how to extend the original Fermat–Euler theorem to all of the elements of such rings with the best possible choice of exponents. The proofs are based on an idempotent technique of Schwarz.

The results are then applied to Dedekind's rings R satisfying the following finiteness condition:

(FN) *For every non-zero ideal* $\mathfrak{I} \subset R$ *the residue class ring* $R/\mathfrak{I}$ *is finite.*

Further specialization of proved results to some special cases of Dedekind's rings R depends then upon a good detailed knowledge of the structure of the group of units of the corresponding residue class ring $R/\mathfrak{I}$. The most known prototypes of such rings are besides $\mathbb{Z}_n$ the algebraic number fields. Amongst these the simplest cases represent the quadratic fields, including one of their oldest representatives, the ring of the Gaussian integers.

The history of the Fermat theorem

$$x^{p-1} \equiv 1 \pmod{p} \qquad (x, p) = 1,\ p \text{ a prime}$$

is well known. Chapter III of Dickson's History [Dic1919] contains a number of interesting details in this direction. As the capacity of a human

* Research supported by the Slovak Academy of Sciences, Grant 363. E-mail: lassak@savba.sk.

† Research supported by the Grant Agency of the Czech Republic, Grant 201/93/2122. E-mail: porubsks@vscht.cz.

0022-314X/96 $18.00

being is limited, it is not surprising that new facts can be found in other sources. So, for instance, Sierpiński [Sie1959, p. 177] mentions that according to Barycz [Bar1954, issue 1, p. 3], this result was discovered by Brożek (1585–1672), professor of the Cracow Academy.

Euler gave several proofs of Fermat's theorem. The third of them was based on the observation [Dic1919, pp. 60–61] which also plays an underlying role in the subsequent lines: If p is a prime and a is any integer not divisible by p, at most $p-1$ of the positive residues $<p$, obtained by dividing $1, a, a^2, \ldots$ by p are distinct. If a^μ, a^ν, where $\mu > \nu$, have the same residue, then $a^{\mu-\nu}-1$ is divisible by p. If λ is the least positive integer for which $a^\lambda - 1$ is divisible by p, then Euler showed that λ divides $p-1$, and consequently $a^{p-1}-1$ is divisible by p.

Since this proof relies only on the fact that every $a<p$ is coprime to p, it was capable of further extension and Euler soon gave an important generalization from the case of a prime p to any integer n:

$$a^{\varphi(n)} \equiv 1 \qquad (\mathrm{mod}\, n),$$

for every a coprime to n.

The next essential generalization was made by Galois [Dic1919, p. 235], who extended it to algebraic number fields. More or less ingenious generalizations were proved later, mostly in two directions: to lower the exponent or to get a congruence holding also for x not coprime to n. To mention two of the most important of them, Lucas [Dic1919, p. 78] replaced the order φ of the multiplicative group of invertible elements $\mathrm{mod}\, n$ by the (group) exponent of this group which is given by the Carmichael function λ. To get a congruence holding for all x, Bachmann [Dic1919, p. 78] multiplies the former congruence by x^σ where σ is the greatest exponent of the prime factors of n.

These generalizations were based on ad hoc ideas, and the idea that the identity 1 and the group of invertible elements $\mathrm{mod}\, n$ are only a special case of an idempotent and a (semi)group belonging to an idempotent totally escaped notice. In 1981 Schwarz [Sch1981] made a detailed analysis of Fermat's theorem from this point of view.

The present work is a direct continuation of the ideas of [Sch1981] with only one difference. In [Sch1981] the author advocates a strictly semigroup point of view. This means that the proofs of his generalizations of the classical Fermat–Euler theorem are based on the idea of exploiting only the multiplicative structure of the ring $\mathbb{Z}/n\mathbb{Z}$ of residue classes $(\mathrm{mod}\, n)$ whenever possible. This point of view is self-evident if one attempts to follow the semigroup theory techniques based on the significant role the idempotents play in the theory of semigroups. Since the Fermat–Euler theorem touches both multiplicative and additive structure of $\mathbb{Z}/n\mathbb{Z}$ we

abandon this puristic semigroup point of view in the present paper. Exploiting the whole ring theoretic structure of rings under consideration we give a ring theoretic analysis of Schwarz's ideas and so we prove the corresponding extension of the Fermat–Euler theorem for finite commutative rings with identity. Then we apply the proved results to Dedekind's rings R satisfying the following finiteness condition:

(FN) *For every non-zero ideal* $\mathfrak{I} \subset R$ *the residue class ring* $R/\mathfrak{I}$ *is finite.*

Specialization of the proved result to some special cases of Dedekind's rings R depends upon a good detailed knowledge of the structure of the group of units of the corresponding residue class rings $R/\mathfrak{I}$. This knowledge is available for the algebraic number fields as well as $\mathbb{Z}_n$. Amongst these the simplest cases represent the quadratic fields, including one of their oldest representatives, the ring of the Gaussian integers. We show how our results can be applied to prove corresponding maximal generalizations of the Fermat–Euler theorem.

1. MULTIPLICATIVE SEMIGROUPS OF FINITE COMMUTATIVE RINGS

1.1. *Idempotents*

Unless the contrary is stated, R always denotes a *finite commutative ring with identity* $1 = 1_R$ and E the set of its idempotents. The set E is nonempty for $0, 1 \in E$ and it is finite.

LEMMA 1.1. *The set* E *endowed with the operations* $\wedge$, $\vee$, $'$ *defined by*

$$x \wedge y = xy$$
$$x \vee y = x + y - xy$$
$$x' = 1 - x,$$

forms a Boolean algebra.

Moreover, on E it is possible define an (partial) ordering

$$x \leqslant y \Leftrightarrow xy = x.$$

An idempotent $e \in E$ is called

primitive if it is an atom in the lattice $(E, \wedge, \vee)$, i.e., if it is minimal in the ordered set $(E \setminus \{0\}, \leqslant)$

maximal if it is maximal in $(E \setminus \{1\}, \leqslant)$.

Two idempotents $e, f \in E$ are called *orthogonal* provided $ef = 0$.

The following two lemmas list some basic properties of primitive and maximal idempotents:

LEMMA 1.2. *Let $e_1, ..., e_n$ be the all primitive idempotents of R. Then*

(i) *$e_1, ..., e_n$ are pairwise orthogonal, i.e.,*

$$e_i e_j = 0 \qquad \text{for} \quad i \neq j.$$

(ii)

$$e_1 + \cdots + e_n = 1. \tag{1.1}$$

(iii) *If $0 \neq f \in E$, then*

$$fe_i = \begin{cases} e_i & \text{if} \quad e_i \leqslant f, \\ 0 & \text{otherwise.} \end{cases} \tag{1.2}$$

(iv) *If $0 \neq f \in E$, then*

$$f = \sum_{\substack{i=1 \\ fe_i = e_i}}^{n} e_i. \tag{1.3}$$

The Boolean algebra $(2^{\{1, ..., n\}}, \cap, \cup, ')$ is isomorphic with Boolean algebra $(E, \wedge, \vee, ')$ via the isomorphism

$$f \mapsto \{i \in \{1, ..., n\};\ fe_i = e_i\}.$$

We use this isomorphism to simplify our notation. If $f \in E$, then define

$$I_f = \{i \in \{1, ..., n\};\ fe_i = e_i\},$$
$$I'_f = \{1, ..., n\} \setminus I_f.$$

Plainly, $I'_f = I_{f'}$ with $f' = 1 - f$, and $I_1 = \{1, ..., n\}$, $I_0 = \varnothing$.

If we adopt the usual convention that a sum over an empty set vanishes, the property (iv) remains true also for the idempotent $f = 0$. We shall similarly understand by an empty product the element 1.

LEMMA 1.3. *Let $e_1, ..., e_n$ be the all primitive idempotents of R. Then*

(i) *$e'_1 = 1 - e_1, ..., e'_n = 1 - e_n$ are all the maximal idempotents in R,*

(ii) *for every $f \in E$ we have*

$$f = \prod_{i \in I'_f} e'_i = \prod_{i \in I'_f} (1 - e_i). \tag{1.4}$$

This means that arbitrary idempotent $f \in E$ can be uniquely written as sum of certain primitives or as the product of some maximal idempotents, respectively.

1.2. *Maximal Semigroups and Maximal Groups*

In this section we shall study in more detail certain aspects of the semigroup structure of the multiplicative semigroups $(R, \cdot)$ of a finite commutative ring R. Namely, we describe its maximal (in the set theoretic meaning) subsemigroups containing only one idempotent and the maximal subgroups of $(R, \cdot)$.

Since R is a finite ring, in each sequence

$$x, x^2, x^3, \ldots \qquad x \in R \tag{1.5}$$

some elements must repeat. If $k = k(x) \in \mathbb{N}$ ($\mathbb{N}$ is the set of positive integers) denotes the least such exponent, for which x^k appears at least twice in (1.5) and $d = d(x)$ is the least exponent with $x^k = x^{k+d}$, then the sequence (1.5) has the form

$$x, x^2, \ldots, x^{k-1}, x^k, \ldots, x^{k+d-1}, x^k, \ldots .$$

THEOREM 1.1 (Frobenius). *For every $x \in R$ the set*

$$\{x^k, \ldots, x^{k+d-1}\} \tag{1.6}$$

forms a cyclic group with respect to the multiplication.

The proof follows using a standard argument that the map $x^l \mapsto i_l$, where $i_l \equiv l \pmod{d}$ is an isomorphism onto the cyclic additive group $\{0, 1, \ldots, d-1\}$. This argument also shows that the identity element $e = x^r$ of the group (1.6) is given by the exponent $r = r(x)$ uniquely determined by the relations

$$k \leqslant r \leqslant k + d - 1 \qquad \text{and} \qquad d \mid r.$$

As a byproduct of this proof we also see that one of generators of the group (1.6) is the element x^{r+1}, i.e.

$$\{x^k, \ldots, x^{k+d-1}\} = \{xe, \ldots, x^d e = e\}.$$

The element e is the unique idempotent of R which belongs to (1.5) what is usually phrased that *the element x belongs to the idempotent e.*

THEOREM 1.2. *Let $e \in E$. Then the set*

$$P^R(e) = \{x \in R;\ x \text{ belongs to } e\}$$

is the largest subsemigroup of $(R, \cdot)$, which except for e contains no other idempotent of R.

Proof. If $x, y \in P^R(e)$, then $x^t = e = y^l$ for some $t, l \in \mathbb{N}$ and the commutativity of the multiplication gives that $(xy)^{tl} = e$. This shows that $P^R(e)$ is closed under multiplication. It can be easily shown that e is the only idempotent in $P^R(e)$.

Let P be a subsemigroup of $(R, \cdot)$ containing e as the only idempotent, and let $x \in P$. Then on the one hand, the sequence $x, x^2, x^3, \ldots$ contains an idempotent, say, $f = x^u$ for some $u \in \mathbb{N}$. Since P contains only one idempotent e, $f = e$. Therefore x belongs to the idempotent e and thus $x \in P^R(e)$. Consequently $P \subset P^R(e)$, and the proof is finished. ∎

The uniquely determined maximal subsemigroup $P^R(e)$ of the previous theorem will be called the *maximal* (*multiplicative*) *semigroup* (*of the ring R*) *belonging to the idempotent $e \in E$*. Note that

$$R = \bigcup_{e \in E} P^R(e).$$

If $e \in E$ is an idempotent in R, then there always exists a subgroup of $(R, \cdot)$ containing e as its identity, e.g. the group $\{e\}$ or the group of Theorem 1.1 provided x belongs to the idempotent e. The ring R is finite, therefore there exists a finite system, say $\{G_\alpha\}_{\alpha \in A}$, of the maximal subgroups of $(R, \cdot)$ amongst the all subgroups of R with identity element e. Since the set

$$\prod_{\alpha \in A} G_\alpha = \left\{ \prod_{\alpha \in A} x_\alpha;\ x_\alpha \in G_\alpha \right\}$$

is again a subgroup of $(R, \cdot)$ with identity e and containing every subgroup of $\{G_\alpha\}_{\alpha \in A}$, the system of the all subgroups of $(R, \cdot)$ with identity e has the (only) maximal element. We shall call this group $G^R(e)$ the *maximal* (*multiplicative*) *subgroup of* $(R, \cdot)$ *belonging to the idempotent* $e \in E$.

The following structural results can be proved:

THEOREM 1.3. *If $e \in E$, then*

(i) $G^R(e) = \{a \in R;\ a = ae \text{ and } e = ab \text{ for some } b \in R\}$

(ii) $G^R(e) = \{a \in P^R(e);\ ae = a\}$.

Proof. The proof of part (i) is obvious. For the proof of (ii) let $G = \{a \in P^R(e); ae = a\}$. Since every element of $G^R(e)$ belongs to the idempotent e, $G^R(e) \subset G$. Conversely, if $a \in G \subset P^R(e)$, then there exists $t > 0$ with $a^t = e$. If $t = 1$, then $a = e \in G^R(e)$; if $t > 1$, then $a \cdot a^{t-1} = e$, so $a \in G^R(e)$. ∎

COROLLARY 1. *If $e \in E$, then*

$$G^R(e) = P^R(e)\, e; \tag{1.7}$$

specifically for $e = 1$ we have $G^R(1) = P^R(1)$.

If $e \in E$, then

$$eR = \{ex; x \in R\}$$

is a ring with identity element e. This observation leads to another characterization of the group $G^R(e)$:

THEOREM 1.4. *If $e \in E$, then*

(i) *$G^R(e)$ is the group of units of eR with respect to the ring multiplication*

(ii)

$$G^R(e) = P^{eR}(e). \tag{1.8}$$

Proof. (i) The set of the all units of the ring eR forms a group with identity e. Since the group $G^R(e)$ is the maximal group with identity e, the group of units of the ring $eR \subset R$ is a subgroup of $G^R(e)$. Conversely, if $x \in G^R(e)$, then x belongs to the idempotent e and $xe = x$. The last equality shows that $x \in eR$ and the first fact implies the existence of such $t \in \mathbb{N}$ that $x^t = e$. If $t = 1$, then $x = e$ and x clearly is a unit in eR. In the case $t > 1$ we have $e = x^t = x \cdot x^{t-1}$ and that x is invertible in eR if $x^{t-1} \in G^R(e)$. But this is true because $x \in G^R(e)$ and $G^R(e)$ as a group is closed under the multiplication. Thus part (i) is proved.

(ii) Here we have

$$\begin{aligned} G^R(e) = P^R(e)\, e &= \{x \in R; x^t = e \text{ for some } t > 0\}\, e \\ &= \{y \in eR; y^t = e \text{ for some } t > 0\} = P^{eR}(e) \end{aligned}$$

and the proof is finished. ∎

The next result will be very useful:

LEMMA 1.4. *If* $e, f \in E$, *then*

$$P^R(e)\, f = P^{fR}(ef). \tag{1.9}$$

Proof. If $x \in P^R(e)\, f$, then $x = yf$ with $y \in R$ and $y^t = e$ for some $t > 0$. Therefore $x = yf \in fR$. Simultaneously we have $x^t = (yf)^t = y^t f = ef$ which shows that $x \in P^{fR}(ef)$ and proves one inclusion.

Conversely, let $x \in P^{fR}(ef)$ and $x^t = ef$. Consider the element $e - ef + x \in R$. Then $(e - ef + x)\, f = xf = x$, the last equality being a consequence of the fact that f is the identity of the ring fR. Moreover, $(e - ef + x)^t = e - ef + x^t = e - ef + ef = e$. Consequently $x = (e - ef + x)\, f \in P^R(e)\, f$ and the equality $P^R(e)\, f = P^{fR}(ef)$ is proved. ∎

This lemma has some interesting corollaries. One of them is another proof of (1.7) which follows from (1.8) and from (1.9) for $e = f$. The next one concerns the *nil-radical*

$$N(R) = \{x \in R;\ x^t = 0 \text{ for some } t > 0\}$$

which is formed by nilpotent elements of R. In fact, nil-radical is the maximal semigroup belonging to the idempotent 0, i.e., $N(R) = P^R(0)$. This gives the next corollary of Lemma 1.4.

COROLLARY 1. *If* $e \in E$, *then*

$$N(eR) = eN(R).$$

Using Lemma 1.4 and (1.8) we get:

THEOREM 1.5. *If* $e, f \in E$, *then*

$$G^R(e)\, f = G^R(ef) \tag{1.10}$$

and consequently for $e = 1$

$$G^R(1)\, f = G^R(f). \tag{1.11}$$

1.3. *Structure of* $P^R(e)$ *and* $G^R(e)$

LEMMA 1.5 (Peirce Decomposition). *Let* $R_1, ..., R_n$ *be ideals of the ring* R. *Then the following statements are equivalent*:

(a) *The ring* R *is the direct sum of the ideals* $R_1, ..., R_n$, *i.e.*,

$$R = R_1 \oplus \cdots \oplus R_n.$$

(b) *Every $r \in R$ is uniquely expressible in the form*

$$r = r_1 + \cdots + r_n, \qquad \text{where} \quad r_i \in R_i.$$

(c) *There exist pairwise orthogonal idempotents $e_1, ..., e_n$ in R such that*

$$e_1 + \cdots + e_n = 1$$

and $R_i = e_i R$ for every $i = 1, ..., n$.

If $e_1, ..., e_n$ are all the primitive idempotents of R, then the statement (ii) of Lemma 1.2 shows that (c) of the previous lemma is satisfied and we get the Peirce decomposition of R

$$R = e_1 R \oplus \cdots \oplus e_n R. \tag{1.12}$$

Consequently, every $r \in R$ is uniquely expressible in the form $r = r_1 + \cdots + r_n$ with $r_i \in e_i R$. Moreover, $r_i = e_i r$ for $i = 1, ..., n$. As noted after corollary of Theorem 1.3, eR is the ring with identity e. This shows that the map

$$\Psi_e : R \to eR, \; x \mapsto ex$$

is a surjective ring homomorphism. If Φ is the ring isomorphism of R onto $e_1 R \times \cdots \times e_n R$ defined by $r \mapsto (e_1 r, ..., e_n r)$, then $\Phi(r) = (\Psi_{e_1}(r), ..., \Psi_{e_n}(r))$.

Properties of maps Ψ_e, $e \in E$, will be useful in finding some decompositions of maximal semigroups $P^R(e)$ and maximal groups $G^R(e)$, respectively.

LEMMA 1.6. *If $e, f \in E$, then*

(i) *The contraction $\Psi_e \mid P^R(f)$ is a semigroup homomorphism of the semigroup $P^R(f)$ onto $P^{eR}(ef)$. Especially, for $e = f$ we get a semigroup homomorphism of $P^R(e)$ onto $G^R(e)$ and the elements of $G^R(e)$ are invariant under this homomorphism.*

(ii) *The contraction $\Psi_e \mid G^R(f)$ is a group homomorphism of the group $G^R(f)$ onto $G^R(ef)$; especially, of a group $G^R(1)$ onto $G^R(e)$.*

For the proof of the second half of (i) take into account (1.7) and (ii) of Theorem 1.3 for the invariantness. In the part (ii) use Theorem 1.4 to see that $G^{eR}(ef) = G^R(ef)$.

For primitive idempotents we have:

LEMMA 1.7. *Let $e_1, e_2, ..., e_n$ be the set of all primitive idempotents of R. Then for each $i = 1, 2, ..., n$ and every idempotent $f \in E$ we have*

$$e_i P^R(f) = P^{e_i R}(e_i f) = \begin{cases} P^{e_i R}(e_i) = G^R(e_i) & \text{if} \quad i \in I_f, \\ P^{e_i R}(0) = N(e_i R) & \text{if} \quad i \in I'_f. \end{cases} \tag{1.13}$$

Proof. The first equality follows from Lemma 1.4 and the rest from (1.2). ▮

THEOREM 1.6. *Let $e_1, e_2, ..., e_n$ be the set of all primitive idempotents of R and $f \in E$. The contraction of Φ to $P^R(f)$ is a semigroup isomorphism onto the cartesian product $P^{e_1 R}(e_1 f) \times \cdots \times P^{e_n R}(e_n f)$.*

Proof. If $x \in P^R(f)$, then Lemma 1.6 implies that $e_i x \in P^{e_i R}(e_i f)$. Since Φ as a ring isomorphism contracted to $P^R(f)$ is an injective semigroup homomorphism, it remains to prove that it is onto.

Let $x_i \in P^{e_i R}(e_i f)$ with $x_i \in e_i R$ and $x_i^{t_i} = e_i f$ for some t_i, $i = 1, ..., n$. It can be easily seen that $x_i x_j = 0$ for $i \neq j$. Let $x = x_1 + \cdots + x_n$. Then

$$\begin{aligned} x^{t_1 \cdots t_n} &= x_1^{t_1 \cdots t_n} + \cdots + x_n^{t_1 \cdots t_n} \\ &= e_1 f + \cdots + e_n f = (e_1 + \cdots + e_n) f. \end{aligned}$$

Thus $x \in P^R(f)$ and moreover $\Phi(x) = (x_1, ..., x_n)$, i.e. the mapping

$$\Phi: P^R(f) \to P^{e_1 R}(e_1 f) \times \cdots \times P^{e_n R}(e_n f)$$

is a surjective semigroup isomorphism, as claimed. ▮

It follows from the previous proof that every $x \in P^R(f)$ can be uniquely written as the sum $x = x_1 + \cdots + x_n$ with $x_i \in P^{e_i R}(e_i f)$ for $i = 1, ..., n$, i.e., that

$$P^R(f) = P^{e_1 R}(e_1 f) \oplus \cdots \oplus P^{e_n R}(e_n f).$$

Using Lemma 1.7 it is possible to simplify the summands as follows:

THEOREM 1.7. *If $f \in E$, then*

$$\begin{aligned} P^R(f) &= \bigoplus_{i \in I_f} G^R(e_i) \oplus \bigoplus_{i \in I'_f} N(e_i R) \\ &= f G^R(1) \oplus (1 - f) N(R) = G^R(f) \oplus N((1 - f) R). \end{aligned} \tag{1.14}$$

For $f = 1$ we get the decomposition of $G^R(1)$ from the theorem

$$P^R(1) = G^R(1) = G^R(e_1) \oplus \cdots \oplus G^R(e_n). \tag{1.15}$$

This decomposition can be also proved using the group isomorphism

$$\Phi: G^R(1) \to G^R(e_1) \oplus \cdots \oplus G^R(e_n).$$

The next special case $f=0$ of Theorem 1.7 yields the direct decomposition of the nil-radical of R

$$P^R(0)=N(R)=N(e_1R)\oplus\cdots\oplus N(e_nR). \tag{1.16}$$

Relations (1.7) and (1.14) or (1.11) with (1.15) imply the following direct decomposition of the group $G^R(f)$:

THEOREM 1.8. *If $f\in R$, then*

$$G^R(f)=\bigoplus_{i\in I_f} G^R(e_i). \tag{1.17}$$

1.4. *Generalizations of Fermat–Euler Theorem*

In Section 1.2 we have established the existence of the least positive numbers $k=k(x)$, $d=d(x)$, and $r=r(x)$ possessing the properties

(i) if $x^{l+h}=x^l$, then $l\geqslant k$ and $d\mid h$,

(ii) x^r is an idempotent of R

for every $x\in R$. In other words:

THEOREM 1.9 (Individual Fermat–Euler Theorem). *If $x\in R$, then*

$$x^{k(x)+d(x)}=x^{k(x)}$$

and the numbers $k(x)$ and $d(x)$ are the least positive numbers with this property.

THEOREM 1.10. *If $x\in R$, then $x^{r(x)}$ is an idempotent of R and the number $r(x)$ is the least positive number with this property.*

Given $e\in E$, define

$$k_e=\max\{k(x);\, x\in P^R(e)\},$$
$$d_e=\text{l.c.m.}\{d(x);\, x\in P^R(e)\}$$

and

$$k_R=\max\{k(x);\, x\in R\},$$
$$d_R=\text{l.c.m.}\{d(x);\, x\in R\}.$$

This leads to the following theorems:

THEOREM 1.11 (Local Fermat–Euler theorem). *If $e \in E$, then for every $x \in P^R(e)$ we have*

$$x^{k_e + d_e} = x^{k_e}.$$

Moreover, the numbers k_e, d_e are the least positive integers such that this equality holds for each $x \in P^R(e)$.

THEOREM 1.12 (Global Fermat–Euler theorem). *For every $x \in R$ we have*

$$x^{k_R + d_R} = x^{k_R}$$

and the numbers k_R, d_R are the least positive integers such that this equality holds for each $x \in R$.

Note that Theorems 1.9, 1.11, and 1.12 correspond to the Lucas–Bachmann generalization of the original Fermat–Euler theorem on three subsemigroup levels of $(R, \cdot)$:

— the least subsemigroup generated by x,

— the maximal subsemigroup belonging to an idempotent of R, and

— the whole multiplicative semigroup of R.

THEOREM 1.13. (i) *If $e \in E$, then for every $x \in P^R(e)$ we have*

$$x^{r_e} = e,$$

where r_e is uniquely determined by the relations $k_e \leqslant r_e \leqslant k_e + d_e - 1$ and $d_e \mid r_e$. The number r_e is the least positive integer such that this is true for each $x \in P^R(e)$.

(ii) *The element x^{r_R} is an idempotent of the ring R for every $x \in R$, where r_R is uniquely determined by the relations $k_R \leqslant r_R \leqslant k_R + d_R - 1$ and $d_R \mid r_R$. The number r_R is the least positive integer such that this is true for each $x \in R$.*

Connections of theorems of the same type as Theorems 1.13, 1.10 with the Fermat–Euler theorem were—to our knowledge—investigated for the first time in [Sch1981].

The rest of the paper is devoted to finding more explicit expressions of the parameters k_e, d_e, r_e and k_R, d_R, r_R in terms of some invariants of e and R, respectively. For this we shall need the next structural result:

THEOREM 1.14. *Let $e_1, ..., e_n \in E$ be the primitive idempotents of R. Then for every $i = 1, ..., n$ we have*

$$e_i R = G^R(e_i) \cup N(e_i R) \tag{1.18}$$

and this union is disjoint.

Proof. Take an $x \in e_i R$. Then there exists $y \in R$ with $x = e_i y$. Since $R = \bigcup_{e \in E} P^R(e)$, the element y belongs to some idempotent, say f, i.e., $y^t = f$ for some $t > 0$. Two cases are possible:

1. If $i \in I_f$, then $e_i f = e_i$ and consequently

$$x^t = (e_i y)^t = e_i y^t = e_i f = e_i,$$

i.e., $x \in P^R(e_i)$. Because $x \in e_i R$, $x \in G^R(e_i)$.

2. If $i \in I'_f$, then $e_i f = 0$ and

$$x^t = (e_i y)^t = e_i y^t = e_i f = 0,$$

i.e., $x \in N(e_i R)$.

This proves (1.18). The fact that the union here is disjoint follows from the fact that $0 \notin G^R(e_i)$ and that no non-zero nilpotent element is a group element. ∎

In [FaM1958] a ring is called *divided* if it has the identity and if every element of R is either invertible or nilpotent. Rings which are direct sums of a finite number of divided subrings are called *semidivided* in this paper. Thus we have proved in the previous theorem that every finite ring with identity is semidivided.

Now we shall investigate more closely the question when an element $x \in R$ or some of its powers belong to a (maximal) subgroup of R. We know from the definition of $k(x)$ for $x \in R$ that $x^{k(x)}$ belongs to a group.

Let $x \in R$ belong to an idempotent f, i.e., $x \in P^R(f)$. We know from (1.14) that $P^R(f) = G^R(f) \oplus N((1-f)R)$, therefore x is a group element if and only if $x \in G^R(f)$ and this is true if and only if $x(1-f) = 0$, i.e. if $xe_i = 0$ for every $i \in I_{1-f} = I_{f'}$.

Now let $x = x_1 + \cdots + x_n$, where if $i \in I_f$, then $x_i \in G^R(e_i)$ and if $i \in I_{f'}$, then $x_i \in N(e_i R)$. Since $x^t = x_1^t + \cdots + x_n^t$, the element x^t belongs to $G^R(f)$ if and only if $x_i^t = 0$ for every $i \in I_{f'}$. Therefore define for $y \in e_i R$

$$v_i(y) = \begin{cases} 1 & \text{if } y \in G^R(e_i), \\ t & \text{if } y \in N(e_i R), \text{ where } t \text{ is minimal with } y^t = 0. \end{cases}$$

Then by the *index* of $x \in R$ we shall understand the number

$$v(x) = \max\{v_i(e_i x);\ i = 1, ..., n\}.$$

Theorem 1.14 shows that $v(x)$ is well-defined for every $x \in R$.

The next result is a consequence of the previous considerations:

THEOREM 1.15 (Farahat–Mirsky [FaM1958]). *Let $x \in R$. Then x^t belongs to a subgroup of $(R, \cdot)$ if and only if $t \geqslant v(x)$.*

COROLLARY 1. *For every $x \in R$ we have $k(x) = v(x)$.*

Proof of the Corollary. Since $x^{k(x)}$ belongs to a group, $k(x) \geqslant v(x)$. On the other hand, if $x^{v(x)}$ belongs to a group, then $x^{v(x)}$ appears more than once in the sequences $x, x^2, ...$ which, owing to the definition of $k(x)$, immediately implies that $k(x) \leqslant v(x)$. ∎

If $x \in G^R(f)$ for some $f \in E$, then $\mu(x)$ will denote the order of x in $G^R(f)$, i.e., $\mu(x)$ is the least positive integer satisfying $x^{\mu(x)} = f$.

If $x \in R$ belongs to the idempotent f, then we know (Theorem 1.1) that $\{x^k, ..., x^{k+d-1}\} = \{xf, ..., x^d f = f\}$ is a cyclic group and $d(x)$ is the least positive integer with $(xf)^{d(x)} = f$. This means that for $x \in P^R(f)$ we have $d(x) = \mu(xf)$. Thus if $x \in G^R(f)$, then $d(x) = \mu(x) = \mu(xf)$ which together implies

$$x^{v(x)+\mu(xf)} = x^{v(x)}.$$

Let

$$\begin{aligned} v^{(i)} &= \max\{v(x);\ x \in e_i R\}, \\ \mu^{(i)} &= \text{l.c.m.}\{\mu(x);\ x \in G^R(e_i)\} \end{aligned} \tag{1.19}$$

for every $i = 1, ..., n$. What are the least positive integers v_f, μ_f for which

$$\begin{aligned} x^{v_f} &\in G^R(f) \qquad \text{for every} \quad x \in P^R(f), \\ x^{\mu_f} &= f \qquad\quad \text{for every} \quad x \in G^R(f)? \end{aligned}$$

Theorem 1.15 implies that $x^t \in G^R(f)$ if and only if $t \geqslant v(x)$, consequently $v_f \geqslant v^{(i)}$ for every $i \in I_{f'}$, i.e.,

$$v_f = \max\{v^{(i)};\ i \in I_{f'}\}. \tag{1.20}$$

Let $x \in G^R(f)$. Then (1.17) implies that $x = \sum_{i \in I_f} x_i$ with $x_i \in G^R(e_i)$. Thus $f = x^{\mu_f} = \sum_{i \in I_f} x_i^{\mu_f}$. On the other hand, $f = \sum_{i \in I_f} e_i$ and because this

decomposition is uniquely determined we have $x_i^{\mu_f} = e_i$ for every $i \in I_f$. Consequently, $\mu(x) \mid \mu_f$ for every $x \in \bigcup_{i \in I_f} G^R(e_i)$, i.e.

$$\mu_f = \text{l.c.m.}\{\mu^{(i)}; i \in I_f\}. \tag{1.21}$$

Numbers μ_f, $f \in E$, have the following property:

LEMMA 1.8. *If $f \in E$, then $\mu_f \mid \mu_1$.*

Proof. If $x \in G^R(f)$, then $1 - f + x \in G^R(1)$ and $x = f(1 - f + 2)$ and

$$x^{\mu_1} = (f(1 - f + x))^{\mu_1} = f \cdot 1 = f,$$

that is $\mu_f \mid \mu_1$. ∎

If we understand the *exponent* of a finite group to be the least positive integer θ such that for every $x \in G$ we have $x^\theta = 1$, the identity of G, then:

COROLLARY 1. *The number μ_f is the exponent of the group $G^R(f)$.*

If analogically to (1.20) and (1.21) we define

$$\begin{aligned} \nu_R &= \max\{\nu_f; f \in E\} = \nu_0, \\ \mu_R &= \text{l.c.m.}\{\mu_f; f \in E\} = \mu_1, \end{aligned} \tag{1.22}$$

then these are the least positive integers such that:

1. x^{ν_R} is an element of a group for every $x \in R$,
2. x^{μ_R} is an idempotent for every $x \in \bigcup_{f \in E} G^R(f)$.

The previous considerations together give the following generalized Fermat–Euler theorems (global and local) which are "computationally easier" in comparison with the Theorems 1.11 and 1.12, because it reduces the determination of the values of $\nu^{(i)}$, $\mu^{(i)}$ for $i = 1, ..., n$ to the knowledge of the values ν_f, μ_f for every $f \in E$. Thus we have:

THEOREM 1.16 (Generalized Fermat–Euler Theorem).

$$\begin{aligned} x^{\nu_f + \mu_f} &= x^{\nu_f} \qquad \textit{for every} \quad x \in P^R(f), \\ x^{\nu_0 + \mu_1} &= x^{\nu_0} \qquad \textit{for every} \quad x \in R. \end{aligned} \tag{1.23}$$

2. PRINCIPAL IDEAL RINGS

In this section we shall specialize the previous results to *commutative principal ideal rings R* with identity which satisfy the condition (FN). Since

every principal ideal ring is a unique factorization ring, the greatest common divisor (a, b) of any two elements $a, b \in R$ exists and is uniquely determined up to a unit.

2.1. *Residue Class Rings*

Let $n \in R$, $n \neq 0$ be an arbitrary fixed element. Then we shall denote the finite residue class ring $R_n = R/(n)$. The symbol $\mathcal{N}(n)$ will denote the cardinality of $R/(n)$ and called the *norm* of n.

If $x \in R$, then

$$[x] = [x]_n = x + (n)$$

will denote the residue class modulo the principal ideal (n) containing x. If $x, y \in R$ with $x \equiv y \pmod{n}$ and $d \mid n$, $d \in R$, then $(d, x) = (d, y)$. This enables us to define $(d, [x]) = (d, x)$ uniquely up to a unit.

Let t be a divisor of n. We say that t is a *unitary divisor* of n if $(t, n/t) = 1$. The unitary divisor d (of n) will be said to be *generated by* t if both t and d are divisible by the same set of irreducible elements of R. The unitary divisor d generated by t will be denoted by $d = \langle t \rangle$.

LEMMA 2.1. *If* $x \in R$, *then*

$$[x] = [ta].$$

where $t = (n, [x])$ *and* $[a] \in G^{R_n}([1])$.

Proof. If $t = (n, [x])$, then $[x] = [tb]$ with $(n/t, [b]) = 1$. Let d be the unitary divisor generated by $(n, [b])$, i.e., $d = \langle (n, [b]) \rangle$. Obviously $d \mid t$. If $a = b + n/d$, then

$$[ta] = \left[t\left(b + \frac{n}{d} \right) \right] = [tb] + [n]\left[\frac{t}{d} \right] = [tb] = [x].$$

We claim that $(n, b + n/d) = 1$. Let p be an irreducible element of R with $p \mid n$. Then one of the following alternatives holds:

1. $p \mid n/d$, then $p \nmid d$ and consequently $p \nmid b$, what implies that $p \nmid b + n/d$.

2. $p \nmid n/d$, then $p \mid d$ and consequently $p \mid b$, what implies that $p \nmid b + n/d$.

Thus $(n, b + n/d) = 1$, i.e. $[a] \in G^{R_n}([1])$. ∎

If $t = (n, [x])$ we say that the element $[x]$ *belongs to the divisor* t.

The next theorem generalizes Theorem 2.1 of [Sch1981].

THEOREM 2.1. *There exists a one-to-one correspondence between unitary divisors of n and idempotents of the residue class ring R_n. More precisely, every idempotent is expressible in the form $[ta]$, where t is a unitary divisor of n and $[a] \in G^{R_n}([1])$ is given by a solution of the congruence*

$$ta \equiv 1 \qquad \left(\mathrm{mod}\ \frac{n}{t}\right). \tag{2.1}$$

Proof. Let $[f] = [ta]$, $[a] \in G^{R_n}([1])$ be an idempotent. Then $[f]^2 = [f]$, i.e., $f^2 \equiv f \pmod{n}$ or

$$t^2a^2 \equiv ta \qquad (\mathrm{mod}\ n),$$

and consequently

$$ta \equiv 1 \qquad \left(\mathrm{mod}\ \frac{n}{t}\right).$$

Thus $(t, n/t) = 1$, i.e., t is a unitary divisor of n.

Conversely, let t be a unitary divisor of n. We show that there is an a with $[a] \in G^{R_n}([1])$ which satisfies (2.1).

Since $(t, n/t) = 1$, there exist $b, c \in R$ with

$$bt + c\frac{n}{t} = 1.$$

In other words, $bt \equiv 1 \pmod{n/t}$ and $(b, n/t) = 1$. Since each solution of (2.1) is expressible in the form

$$b + \frac{n}{t}k, \qquad k \in R,$$

the first step is to find a $k \in R$ with $(b + (n/t)k, n) = 1$. To prove that the element $k = t/\langle (t, b) \rangle$ satisfies this condition we shall proceed as in the proof of Lemma 2.1. Let $p \in R$ be an irreducible element with $p \mid n$. Then either

$$p \left| \frac{n}{\langle (t, b) \rangle} \left(= \frac{n}{t}k \right) \right.; \text{ in this case } p \nmid \langle (t, b) \rangle,$$

$$\text{consequently } p \nmid b, \text{ i.e., } p \nmid b + \frac{n}{\langle (t, b) \rangle},$$

or

$$p \nmid \frac{n}{\langle (t, b) \rangle} \left(= \frac{n}{t} k \right); \text{ in this case } p \mid \langle (t, b) \rangle,$$

$$\text{consequently } p \mid b, \text{ i.e., } p \nmid b + \frac{n}{\langle (t, b) \rangle}.$$

Thus in both cases

$$[a] = \left[b + \frac{n}{\langle (t, b) \rangle} \right] \in G^{R_n}([1]),$$

as required.

It remains to show that if $[a], [b] \in G^{R_n}([1])$ with $ta \equiv 1 \pmod{(n/t)}$ and $tb \equiv 1 \pmod{(n/t)}$, then $[ta] = [tb]$. However, $ta - tb \equiv t(a-b) \equiv 0 \pmod{(n/t)}$ then $a \equiv b \pmod{(n/t)}$, i.e. $ta \equiv tb \pmod{n}$. ∎

If $[f] = [ta]$, $[a] \in G^{R_n}([1])$ is an idempotent, then we say that $[f]$ is the *idempotent belonging to the* (*unitary*) *divisor* t.

Suppose that

$$n = a p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r},$$

where a is a unit and $p_1, ..., p_r$ are irreducible nonassociated elements of R and $u_1, ..., u_r$ are positive integers.

For a divisor t of n define

$$J_t = \{ j \in \{1, 2, ..., r\}; p_j \mid t \}.$$

The number of unitary divisors of n is 2^r and every of them is of the form

$$t = \prod_{j \in J_t} p_j^{u_j}.$$

Plainly, $[0]$ is the idempotent belonging to the divisor $t = n$ and $[1]$ is the idempotent belonging to the divisor $t = 1$. It can be easily verified that idempotent $[e_i]$ belonging to the divisor

$$n_i = \frac{n}{p_i^{u_i}} = \prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{u_j}$$

is primitive for every $i = 1, ..., r$.

Some other properties of idempotents are collected in the next result:

LEMMA 2.2. *Let* $[e]$ *and* $[f]$ *be idempotents of* R_n *belonging to the unitary divisors* t *and* s *of* n. *Then*

(i) $I_{[e]} = J_{n/t}$.

(ii) $[e] \wedge [f] = [e][f]$ *is the idempotent belonging to the unitary divisor* $d = \text{l.c.m.}(t, s)$ *and* $J_d = J_t \cup J_s$.

(iii) $[e] \vee [f]$ *is the idempotent belonging to the divisor* $d = (t, s)$ *and* $J_d = J_t \cap J_s$.

(iv) $[e]'$ *is the idempotent belonging to the unitary divisor* $d = n/t$ *and* $J_d = \{1, ..., r\} \setminus J_t$.

Proof. We only prove the part (i); the remaining parts are then its consequences.

Let $[e]$ be the idempotent belonging to the divisor t. Then $i \in J_{[e]}$ if and only if $[e_i e] = [e_i]$, i.e., if $[e_i e] \neq [0]$. On the other hand, $[e_i e] = [0]$ if and only if $p_i \mid t$. Thus $J_t = I_{[e]'}$ or $J_{n/t} = I_{[e]}$. ∎

Lemma 2.1 implies the decomposition of the residue class ring R_n:

THEOREM 2.2.

$$R_n = \bigcup_{t \mid n} [t]\, G^{R_n}([1]) \tag{2.2}$$

and this union is disjoint.

For the maximal semigroup $P^{R_n}([f])$ we have:

THEOREM 2.3. *Let* $[f] \in R_n$ *be the idempotent belonging to the unitary divisor* d *of* n. *Then*

$$P^{R_n}([f]) = \bigcup_{\substack{t \mid d \\ \langle t \rangle = d}} [t]\, G^{R_n}([1]). \tag{2.3}$$

Proof. Let $[x] \in R_n$ belong to the divisor $t = \prod_{j \in J_t} p_j^{v_j}$, where $1 \leqslant v_j \leqslant u_j$, $j \in J_t$. Then

$$\langle t \rangle = d = \prod_{j \in J_t} p_j^{u_j}$$

and let

$$\sigma = \max_{j \in J_t} \left\lceil \frac{u_j}{v_j} \right\rceil,$$

where $\lceil w \rceil$ denotes the upper integer function, i.e. the least integer z with $w \leqslant z$. Since $[f] = [da]$, $[a] \in G^{R_n}([1])$ is the idempotent belonging to the unitary divisor d, then

$$[x]^{\sigma} = [db] = [da][a]^{-1}[b] = [f]([a]^{-1}[b]).$$

If, moreover, τ is the order of the group $G^{R_n}([1])$, then $[x]^{\sigma\tau} = [f]$, i.e., $[x]$ belongs to the idempotent $[f]$.

$$[x] \in P^{R_n}([f]).$$

In the opposite direction, let $[x] \in P^{R_n}([f])$ with $[x] = [ty]$, $[y] \in G^{R_n}([1])$. This means that there exists a positive integer l with $[x]^l = [f]$, i.e.,

$$[da] = [f] = [x]^l = [t]^l [y]^l,$$

and thus t generates the unitary divisor d. ∎

For the maximal group belonging to the idempotent $[f] = [da]$ of the ring R we get from (1.11):

THEOREM 2.4. *Let $[f] \in R_n$ be the idempotent belonging to the unitary divisor d of n. Then*

$$G^{R_n}([f]) = [d]\, G^{R_n}([1]). \tag{2.4}$$

Our next aim is to find a more explicit expression for $v_i([x])$ for $[x] \in [e_i] R_n$.

Let $[e_i]$ be primitive idempotent belonging to the unitary divisor n_i and let $[x] \in [e_i] R_n$, i.e. $[x] = [e_i y]$ with $[y] \in R_n$. Let $[y] = [da]$, where $d = (n, [y])$ and $[a] \in G^{R_n}([1])$. Plainly, $[x]$ is nilpotent if and only if $p_i \mid d$. Let v_i be the highest power of p_i dividing d. Suppose that $v_i > 0$. Then $[x]^{\theta} = [0]$ if and only if $p_i^{u_i} \mid d^{\theta}$ which in turns gives that $\theta \geqslant \lceil u_i/v_i \rceil$. Therefore $v_i([x]) = \lceil u_i/v_i \rceil$ provided $p_i \mid d$, and $v_i([x]) = 1$ otherwise. This together implies:

THEOREM 2.5 (Farahat–Mirsky [FaM1958]). *Let $[x] \in R_n$ be an element belonging to the divisor $d = \prod_{j \in J_d} p_j^{v_j}$, where $1 \leqslant v_j \leqslant u_j$ for every $j \in J_d$. Then*

$$v([x]) = \begin{cases} 1 & \text{if} \quad d = 1 \ (J_d = \varnothing), \\ \max_{j \in J_d} \lceil u_j/v_j \rceil & \text{otherwise.} \end{cases} \tag{2.5}$$

These results enable us to determine explicitly the values of

$$v^{(i)} = \max\{v([x]);\ [x] \in [e_i] R_n\}.$$

If $[x] \in [e_i]\, R_n$, then $[x] = [e_i y] = [n_i][p_i^{v_i}][a]$ with $0 \leqslant v_i \leqslant u_i$ and $[a] \in G^{R_n}([1])$. Thus

$$v^{(i)} = \max\{v([x]);\, [x] \in [e_i]\, R_n\}$$
$$= \max\left\{\left[\frac{u_i}{v_i}\right];\, v_i = 1, ..., u_i\right\} = u_i.$$

Let $[f] \in R_n$ be the idempotent belonging to the divisor d. Then the definition (1.20) and $I_{f'} = J_d$ yield

$$v_{[f]} = \max_{i \in I_{[f]'}} v^{(i)} = \max_{i \in I_{[f]'}} u_i = \max_{j \in J_d} u_j. \tag{2.6}$$

Especially, for $[f] = [0]$ we get

$$v_{[0]} = \max_{i \in \{1, ..., r\}} v^{(i)} = v_{R_n}. \tag{2.7}$$

For the next result we shall need the following function connected with the factorization into irreducible elements. If $m = q_1^{w1} \cdots q_s^{ws}$ is the decomposition of an element into irreducible nonassociated elements in a unique factorization ring S, then define

$$H^S(m) = \max\{w_i;\, i \in \{1, ..., s\}\}.$$

Consequently, if $[f] \in R_n$ is the idempotent belonging to the divisor d and R is a unique factorization ring, then

$$v_{[f]} = H^R(d)$$

and

$$v_{[0]} = v_{R_n} = H^R(n)$$

and the following results are true:

THEOREM 2.6. *Let $[f]$ be the idempotent in R_n belonging to the unitary divisor d of n. Then*

(i) *The element $[x]^{H^R(d)}$ belongs to $G^{R_n}([f])$ for every $[x] \in P^{R_n}([f])$.*

(ii) *The element $[x]^{H^R(n)}$ belongs to a group for every $[x] \in R_n$.*

The numbers $H^R(d)$ and $H^R(n)$ are the least positive integers possessing these properties.

The previous results determine the values of the function v; the next results are useful for determination of the values μ.

THEOREM 2.7. *Let* $[f]=[f]_n \in R_n$ *be the idempotent belonging to the unitary divisor* t *of* n. *Then the finite commutative rings* $R_{n/t}$ *and* $[f]_n R_n$ *with identities* $[1]_{n/t}$, $[f]_n$, *respectively are isomorphic.*

Proof. Let $[f]_n$ be the idempotent belonging to the divisor t. The set $[f]_n R_n$ forms a finite commutative ring with identity $[f]_n$. Define the map θ: $R_{n/t} \to [f]_n R_n$ as follows

$$\theta([x]_{n/t}) = [f]_n [x]_n = [fx]_n.$$

To show that the map θ is well defined take x, y with $[x]_{n/t} = [y]_{n/t}$. Then $x \equiv y \pmod{n/t}$ and multiplication of this congruence by f gives $fx \equiv fy \pmod{n}$, i.e., $[fx]_n = [fy]_n$.

The next property to prove is the injectivity of θ. If $[fx]_n = [fy]_n$, then $[x]_{n/t} = [y]_{n/t}$, and θ is really injective. The surjectivity is also easy to prove for $[fx]_n = \theta([x]_{n/t})$.

It remains to prove that θ is a ring homomorphism. Given $[x]_{n/t}$, $[y]_{n/t} \in R_{n/t}$, we have

$$\begin{aligned}\theta([x]_{n/t} + [y]_{n/t}) &= [f]_n ([x]_n + [y]_n) = [fx]_n + [fy]_n \\ &= \theta([x]_{n/t}) + \theta([y]_{n/t}),\\ \theta([x]_{n/t} \cdot [y]_{n/t}) &= [f]_n ([x]_n \cdot [y]_n) = [f]_n [f]_n [x]_n [y]_n \\ &= [fx]_n [fy]_n = \theta([x]_{n/t}) \cdot \theta([y]_{n/t}).\end{aligned}$$

Moreover, $\theta([1]_{n/t}) = [f]_n [1]_n = [f]_n$, i.e. the unity is mapped onto the unity. ∎

COROLLARY 1. *Let* $[f]=[f]_n \in R_n$ *be the idempotent belonging to the unitary divisor* t *of* n. *Then the unit groups* $G^{R_{n/t}}([1]_{n/t})$ *and* $G^{[f]_n R_n}([f]_n)$ *are isomorphic.*

The proof of this corollary follows from the next lemma and Theorem 1.4.

LEMMA 2.3. *Let* R, S *be commutative rings with identities* 1_R *and* 1_S, *respectively. Let* θ: $R \to S$ *be a ring isomorphism with* $\theta(1_R) = 1_S$. *Then the contraction* $\theta \mid G^R(1_R)$ *is a group isomorphism of the unit groups* $G^R(1_R)$ *and* $G^S(1_S)$.

Proof. Given $x \in G^R(1_R)$, there exists its multiplicative inverse $x^{-1} \in G^R(1_R)$ and

$$1_S = \theta(1_R) = \theta(xx^{-1}) = \theta(x)\,\theta(x^{-1}).$$

Consequently $\theta(x) \in G^S(1_S)$, i.e., the map $\theta \mid G^R(1_R)$ is into the group $G^S(1_S)$. Since θ is a ring isomorphism, $\theta \mid G^R(1_R)$ is an infective group homomorphism of $G^R(1_R)$ into $G^S(1_S)$. It remains to prove that it is also surjective. If $y \in G^S(1_S)$ there exists an $y^{-1} \in G^S(1_S)$ and $a, b \in R$ with $\theta(a) = y$ and $\theta(b) = y^{-1}$. Then

$$\theta(1_R) = 1_S = yy^{-1} = \theta(a)\,\theta(b) = \theta(ab).$$

The injectivity of θ implies that $ab = 1_R$ and thus $a, b \in G^R(1_R)$, i.e., $\theta \mid G^R(1_R)$ is surjective. ∎

COROLLARY 2. *If* $[e_i]$, $i = 1, ..., r$, *are the primitive idempotents of* R_n, *then*

$$G^{R_n}([1]_n) \simeq G^{R_{p_i^{u_i}}}([1]_{p_i^{u_i}}).$$

The final determination of the values $\mu^{(i)}$, $\mu_{[f]}$, and $\mu_{R_n} = \mu_{[1]}$ is thus reduced to detailed knowledge of the structure of groups $G^{R_{p^u}}([1]_{p^u})$, where p is an arbitrary irreducible element of R and $u > 0$.

2.2. *The Ring* $\mathbb{Z}_n$

Let $\mathbb{Z}$ be the ring of integers and $n \in \mathbb{Z}$, $n \neq 0$, then the results of the previous Section 2.1 and the part 1 can be applied to the finite ring $\mathbb{Z}_n = \mathbb{Z}/(n)$. In this case $\mathcal{N}(n) = n$.

Let $n = p_1^{u_1} \cdots p_r^{u_r}$, where p_i are distinct primes and $u_i > 0$, $i = 1, ..., r$. Let $[f] \in \mathbb{Z}_n$ be the idempotent belonging to the unitary divisor d of n. We showed in the previous section that

$$\begin{aligned} v_{[f]} &= \max_{j \in J_d} u_j = H(d), \\ v_{\mathbb{Z}_n} = v_{[0]} &= \max_{j \in \{1, ..., r\}} u_j = H(n). \end{aligned} \tag{2.8}$$

A well known result (see e.g. [Cro1983] or [Has1950]) says (here and in the theorems of this type we mean by $\mathbb{Z}_n$ the additive group of $\mathbb{Z}_n$):

THEOREM 2.8. *If* p *is a prime number in* $\mathbb{Z}$ *and* $u > 0$. *then*

$$G^{\mathbb{Z}_{p^u}}([1]_{p^u}) \simeq \begin{cases} \mathbb{Z}_1 & \text{if } p = 2, \quad u = 1, \\ \mathbb{Z}_2 & \text{if } p = 2, \quad u = 2, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{u-2}} & \text{if } p = 2, \quad u > 2, \\ \mathbb{Z}_{p^u - p^{u-1}} & \text{if } p > 2. \end{cases}$$

This theorem enables us first to determine the values $\mu^{(i)}$ and then also the values $\mu_{[f]}, \mu_{\mathbb{Z}_n}$.

It is known that the exponent of the unit group $G^{\mathbb{Z}_m}([1]_m)$, where $m \in \mathbb{Z}$, $m \neq 0$, is given by the *Carmichael function* λ defined by

$$\lambda(m) = \begin{cases} 1 & \text{if} \quad m = 1, \\ 2^{u-2} & \text{if} \quad m = 2^u, \quad u > 2, \\ \varphi(m) & \text{if} \quad m = 2, 4, \text{ or } p^u \text{ for odd prime } p, \\ \text{l.c.m.}\{\lambda(p_i^{u_i}); i = 1, ..., r\} & \text{if} \quad m = p_1^{u_1} \cdots p_r^{u_r}, \end{cases}$$

where φ is the Euler function. Thus we get:

THEOREM 2.9. *For every* $j = 1, ..., r$,

$$\mu^{(j)} = \lambda(p_j^{u_j}) = \begin{cases} 1 & \text{if} \quad p_j = 2, \quad u_j = 1, \\ 2 & \text{if} \quad p_j = 2, \quad u_j = 2, \\ 2^{u_j - 2} & \text{if} \quad p_j = 2, \quad u_j > 2, \\ p_j^{u_j} - p_j^{u_j - 1} & \text{if} \quad p_j > 2. \end{cases}$$

If $[f] \in \mathbb{Z}_n$ is the idempotent belonging to the divisor d of n, then (1.21) and (1.22) yield

$$\begin{aligned} \mu_{[f]} &= \text{l.c.m.}\{\mu^{(i)}; i \in I_{[f]}\} = \text{l.c.m.}\{\mu^{(j)}; j \in J_{n/d}\} = \lambda\left(\frac{n}{d}\right), \\ \mu_{\mathbb{Z}_n} &= \mu_{[1]} = \text{l.c.m.}\{\mu^{(j)}; j \in \{1, ..., r\}\} = \lambda(n). \end{aligned} \tag{2.9}$$

We thus arrive at our starting result previously proved by Schwarz:

THEOREM 2.10 (Schwarz [Sch1981]). *Let* $[f]$ *be the idempotent of the ring* $\mathbb{Z}_n$ *belonging to the unitary divisor* d *of* n. *Then*

$$\begin{aligned} [x]^{H(d) + \lambda(n/d)} &= [x]^{H(d)} \qquad \textit{for every} \quad [x] \in P^{\mathbb{Z}_n}([f]), \\ [x]^{H(n) + \lambda(n)} &= [x]^{H(n)} \qquad \textit{for every} \quad [x] \in \mathbb{Z}_n. \end{aligned}$$

The numbers $H(d)$, $H(n)$ *and* $\lambda(n/d)$, $\lambda(n)$ *are the least positive integers for which equalities hold.*

2.3. *Gaussian Integers*

Let $\mathcal{G} = \{a + bi; a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers. If $\eta \in \mathcal{G}$, $\eta \neq 0$, then the residue class ring $\mathcal{G}_\eta = \mathcal{G}/(\eta)$ is finite and its cardinality equals $\mathcal{N}(\eta) = \eta\bar{\eta}$, where $\bar{\eta}$ denotes the complex conjugate of η. Since $\mathcal{G}$ is a Euclidean ring, it is a unique factorization ring and thus $\mathcal{G}$ allows a unique factorization

$$\eta = \kappa \beta_1^{u_1} \cdots \beta_r^{u_r} \tag{2.10}$$

into irreducible non-associated elements β_j, $j=1, ..., r$, for every $\eta \in \mathscr{G}$, where κ is a unit. Thus we can use all the results of Section 2.1 and part 1. We saw that to the determination of the values $\mu^{(j)}$ we need the knowledge of the structure of the unit group $G^{\mathscr{G}_{\beta^u}}([1]_{\beta^u})$ of the ring $\mathscr{G}_{\beta^u}$, where β is irreducible element of $\mathscr{G}$ and $u>0$.

The characterization of the irreducible elements of $\mathscr{G}$ is a well-known result (see, e.g., [Cro1983]):

LEMMA 2.4. *A $\beta \in \mathscr{G}$ is irreducible if and only if one of the following conditions is satisfied*:

1. $\beta = \pi$, *where* $\pi\bar{\pi} = q$ *and* q *is a rational prime such that* $q \equiv 1 \pmod 4$,
2. $\beta = p$, *where* p *is a rational prime with* $p \equiv 3 \pmod 4$,
3. $\beta = 1+i$.

The structure of the unit group $G^{\mathscr{G}_{\beta^u}}([1]_{\beta^u})$ for every of these three types of irreducible elements of $\mathscr{G}$ is given in the next theorem:

THEOREM 2.11 (Cross [Cro1983]). *Let β be an irreducible element of $\mathscr{G}$ and $u \in \mathbb{N}$, $u>0$. Then*

$$G^{\mathscr{G}_{\beta^u}}([1]_{\beta^u}) \simeq \begin{cases} \mathbb{Z}_{q^u - q^{u-1}} & \text{if } \beta=\pi,\ q=\pi\bar{\pi},\ q\equiv 1 \pmod 4,\ q \text{ a prime}, \\ \mathbb{Z}_{p^{u-1}} \times \mathbb{Z}_{p^{u-1}} \times \mathbb{Z}_{p^2-1} & \text{if } \beta=p,\ p\equiv 3 \pmod 4,\ p \text{ a prime}, \\ \mathbb{Z}_1 & \text{if } \beta=1+i,\ u=1, \\ \mathbb{Z}_2 & \text{if } \beta=1+i,\ u=2, \\ \mathbb{Z}_4 & \text{if } \beta=1+i,\ u=3, \\ \mathbb{Z}_2 \times \mathbb{Z}_4 & \text{if } \beta=1+i,\ u=4, \\ \mathbb{Z}_{2^{v-1}} \times \mathbb{Z}_{2^{v-2}} \times \mathbb{Z}_4 & \text{if } \beta=1+i,\ u=2v,\ v\geqslant 3, \\ \mathbb{Z}_{2^{v-1}} \times \mathbb{Z}_{2^{v-1}} \times \mathbb{Z}_4 & \text{if } \beta=1+i,\ u=2v+1,\ v\geqslant 2. \end{cases}$$

Now it is easy to write down the basic relations for the analogue of the Carmichael function for Gaussian integers, which are in our notation expressed through the values $\mu^{(j)}$, $j=1, ..., r$. We have:

THEOREM 2.12. *For every* $j=1, ..., r$,

$$\mu^{(j)} = \begin{cases} q^{u_j} - q^{u_j-1} & \text{if } \beta_j=\pi,\ q=\pi\bar{\pi},\ q\equiv 1 \pmod 4,\ q \text{ a rational prime}, \\ p^{u_j-1}(p^2-1) & \text{if } \beta_j=p,\ p\equiv 3 \pmod 4,\ p \text{ a rational prime}, \\ 1 & \text{if } \beta_j=1+i,\ u_j=1, \\ 2 & \text{if } \beta_j=1+i,\ u_j=2, \\ 4 & \text{if } \beta_j=1+i,\ u_j=3, 4, 5, \\ 2^{v-1} & \text{if } \beta_j=1+i,\ u_j=2v \text{ or } u_j=2v+1,\ v\geqslant 3. \end{cases}$$

Proof. To the proof note that if the unit group $G^{\mathscr{G}_{\beta_j^{\mu_j}}}([1]_{\beta_j^{\mu_j}})$ is isomorphic with the additive group $\mathbb{Z}_m$, then $\mu^{(j)} = m$ and if it is isomorphic with the product of additive groups $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, then $\mu^{(j)} =$ l.c.m.(m_1, m_2). ∎

Let $[\varepsilon] \in \mathscr{G}_\eta$ be the idempotent belonging to the unitary divisor τ of η. Then according to the relations (1.21) and (1.22) we have:

$$\mu_{[\varepsilon]} = \text{l.c.m.}\{\mu^{(j)};\ j \in I_{[\varepsilon]}\} = \text{l.c.m.}\{\mu^{(j)};\ j \in J_{\eta/\tau}\},$$
$$\mu_{\mathscr{G}_\eta} = \mu_{[1]} = \text{l.c.m.}\{\mu^{(j)};\ j \in \{1, ..., r\}\}.$$

And the generalization of the Fermat–Euler theorem for Gaussian integers follows:

THEOREM 2.13 (Generalized Fermat–Euler Theorem for Gaussian Integers). *Let $[\varepsilon]$ be the idempotent of the ring $\mathscr{G}_\eta$ belonging to the unitary divisor τ. Then*

$$[x]^{H^{\mathscr{G}}(\tau)+\mu_{[\varepsilon]}} = [x]^{H^{\mathscr{G}}(d)} \qquad \textit{for every} \quad [x] \in P^{\mathscr{G}_\eta}([\varepsilon]),$$
$$[x]^{H^{\mathscr{G}}(\eta)+\mu_{[1]}} = [x]^{H^{\mathscr{G}}(\eta)} \qquad \textit{for every} \quad [x] \in \mathscr{G}_\eta.$$

The numbers $H^{\mathscr{G}}(\tau)$, $H^{\mathscr{G}}(\eta)$ and $\mu_{[\varepsilon]}$, $\mu_{[\varepsilon]}$ are the least positive integers for which these identities are true.

3. DEDEKIND RINGS

Integral ring R with identity is called the *Dedekind ring*, if its every proper (distinct from (0) and R) ideal $\mathfrak{I}$ is a finite product of prime ideals.

The other most used characterization of Dedekind rings is in the next lemma:

LEMMA 3.1. *Let R be an integral ring with identity. Then R is a Dedekind ring if and only if it satisfies the following conditions*:

1. *R is Noetherian, i.e., every one of its ideals is of a finite type,*
2. *every proper prime ideal is maximal,*
3. *R is integrally closed.*

For our later applications the most important properties of Dedekind rings are:

LEMMA 3.2. *A residue class ring $R/\mathfrak{I}$ of a Dedekind ring R with respect to the ideal $\mathfrak{I}$ is again a Dedekind ring.*

LEMMA 3.3. *Every proper ideal $\mathfrak{I}$ of a Dedekind ring R may be uniquely (up to the order of the factors) expressed in the form*

$$\mathfrak{I} = \mathfrak{P}_1^{u_1} \cdots \mathfrak{P}_r^{u_r}, \tag{3.1}$$

where $\mathfrak{P}_1, ..., \mathfrak{P}_r$ are distinct prime ideals of R and $u_i > 0$, $i = 1, ..., r$.

Similarly to the previous section we can define the function $\mathscr{H}$ on proper ideals of a Dedekind ring R

$$\mathscr{H}^R(\mathfrak{I}) = \max\{u_i;\ i \in \{1, ..., r\}\}$$

if (3.1) is the decomposition of $\mathfrak{I}$ into the product of prime ideals. This function is obviously an extension of the function H defined in the previous part. Plainly, if R is a unique factorization ring, then it is also Dedekind and for $m \in R$ we have

$$H^S(m) = \mathscr{H}^S((m)).$$

As usual, we say that an ideal $\mathfrak{U}$ divides an ideal $\mathfrak{B}$ if there exists an ideal $\mathfrak{C}$ with $\mathfrak{B} = \mathfrak{A}\mathfrak{C}$. We express this by the usual notation $\mathfrak{A} \mid \mathfrak{B}$. It is a routine exercise to show that $\mathfrak{A} \mid \mathfrak{B}$ if and only if $\mathfrak{A} \supset \mathfrak{B}$.

The greatest common divisor $(\mathfrak{A}, \mathfrak{B})$ of two ideals $\mathfrak{A}$ and $\mathfrak{B}$ is the ideal $\mathfrak{A} + \mathfrak{B} = \{a + b;\ a \in \mathfrak{A},\ b \in \mathfrak{B}\}$ as the least (with respect to the set inclusion) ideal containing both ideals $\mathfrak{A}$ and $\mathfrak{B}$. The ideals $\mathfrak{A}$ and $\mathfrak{B}$ are coprime if $(1) = R$ is their gcd.

If $x, y \in R$ and $\mathfrak{A}$ is an ideal in R, then we write $x \equiv y \pmod{\mathfrak{A}}$ provided $x - y \in \mathfrak{A}$.

LEMMA 3.4 (Chinese Remainder Theorem). *Let R be a Dedekind ring. Then given a finite number of coprime ideals $\mathfrak{I}_1, ..., \mathfrak{I}_n$ and elements $x_1, ..., x_n \in R$, the system of congruences $x \equiv x_i \pmod{\mathfrak{I}_i}$, $i = 1, ..., n$, admits a common solution $x \in R$.*

3.1. *Residue Class Rings of Dedekind Rings*

We shall tacitly suppose that all Dedekind rings R under consideration satisfy the following condition

(FN) *For every non-zero ideal $\mathfrak{I} \subset R$ the residue class ring $R/\mathfrak{I}$ is finite.*

Let $\mathfrak{I}$ be a non-zero ideal of R. We shall denote the residue class ring $R/\mathfrak{I}$ by $R_{\mathfrak{I}}$ and its elements by $[x] = [x]_{\mathfrak{I}} = x + \mathfrak{I}$ for $x \in R$. The norm $\mathscr{N}(\mathfrak{I})$ of an ideal $\mathfrak{I}$ is defined as the cardinality of the residue class ring $R_{\mathfrak{I}}$.

First of all we have to transfer some notions of part 2 to the Dedekind rings setting. Therefore, we define the relation $\sim$ on the ring $R_{\mathfrak{I}}$ as follows:

$$[x] \sim [y] \Leftrightarrow ((x), \mathfrak{I}) = ((y), \mathfrak{I}), \tag{3.2}$$

where $((x), \mathfrak{I})$ stands for the gcd of ideals (x) and $\mathfrak{I}$. The relation $\sim$ is well defined, because the ideal $((x), \mathfrak{I})$ does not depend on the choice of the representative of the class $[x]$. Clearly, $\sim$ is a equivalence relation on $R_{\mathfrak{I}}$.

If $[x] \in R_{\mathfrak{I}}$ and $\mathfrak{T} = ((x), \mathfrak{I})$, then we say that $[x]$ *belongs to the divisor* $\mathfrak{T}$ of $\mathfrak{I}$. The set of all classes $[x]$ which belong to the divisor $\mathfrak{T}$ of $\mathfrak{I}$ will be denoted by $[\mathfrak{T}]_{\sim}$. These sets $[\mathfrak{T}]_{\sim}$, where the ideal $\mathfrak{T}$ is a divisor of the ideal $\mathfrak{I}$, are actually equivalence classes of the factor set $R_{\mathfrak{I}}/\sim$. This proves the next result analogical to Theorem 2.2:

THEOREM 3.1. *We have that*

$$R_{\mathfrak{I}} = \bigcup_{\mathfrak{T} \mid \mathfrak{I}} [\mathfrak{T}]_{\sim} \tag{3.3}$$

and this union is disjoint.

The unit group $G^{R_{\mathfrak{I}}}([1])$ of the ring $R_{\mathfrak{I}}$ is formed by those elements $[x]$ which belong to the divisor $(1) = R$, i.e., $G^{R_{\mathfrak{I}}}([1]) = [(1)]_{\sim}$.

In our discussion in part 2 the notion of a unitary divisor played an important role. We extend this notion in the following way. Let an ideal $\mathfrak{T}$ divide the ideal $\mathfrak{I}$. Then the ideal $\mathfrak{T}$ is called the *unitary divisor* of $\mathfrak{I}$, if $(\mathfrak{T}, \mathfrak{I}/\mathfrak{T}) = (1)$. Moreover, an ideal $\mathfrak{D}$ is called the *unitary divisor generated by the divisor* $\mathfrak{T}$ of $\mathfrak{I}$ provided that $\mathfrak{D}$ is a unitary divisor of the ideal $\mathfrak{I}$ and that $\mathfrak{D}$ is divisible by exactly the same prime ideals of the ring R as the ideal $\mathfrak{T}$. We shall denote it by $\mathfrak{D} = \langle \mathfrak{I} \rangle$.

If (3.1) is the factorization of an ideal $\mathfrak{I}$ into distinct prime ideals $\mathfrak{P}_1, ..., \mathfrak{P}_r$, $u_i > 0$, $i = 1, ..., r$, then given a divisor $\mathfrak{T}$ of the ideal $\mathfrak{I}$, define

$$J_{\mathfrak{T}} = \{ i \in \{1, ..., r\}; \mathfrak{P}_i \mid \mathfrak{T} \}.$$

In the next lines we shall clarify the question about the relation between unitary divisors of the ideal $\mathfrak{I}$ and idempotents of the residue class ring $R_{\mathfrak{I}}$.

According to the definition of idempotents an element $[x] \in R_{\mathfrak{I}}$ is an idempotent if $[x]^2 = [x]$, i.e., $x^2 \equiv x \pmod{\mathfrak{I}}$. This congruence is equivalent to the system of congruences

$$x(x-1) \equiv 0 \pmod{\mathfrak{P}_i^{u_i}}, \qquad i = 1, ..., r.$$

Since the elements x, $x-1$ are coprime ($(x) + (x-1) = (1)$), we have either $x \equiv 0 \pmod{\mathfrak{P}_i^{u_i}}$ or $x \equiv 1 \pmod{\mathfrak{P}_i^{u_i}}$ for every $i \in \{1, ..., r\}$. This implies that $[x]$ belongs to a divisor which is unitary.

On the other hand, let an ideal $\mathfrak{D}$ be a unitary divisor of $\mathfrak{I}$ and consider the following system of congruences:

$$\begin{aligned} x &\equiv 0 \pmod{\mathfrak{P}_i^{u_i}} \qquad \text{for} \quad i \in J_{\mathfrak{D}}, \\ x &\equiv 1 \pmod{\mathfrak{P}_i^{u_i}} \qquad \text{for} \quad i \in \{1, ..., r\} \setminus J_{\mathfrak{D}}. \end{aligned} \tag{3.4}$$

The Chinese Remainder Theorem 3.4 shows that this system is solvable in R. Moreover, if $y, z \in R$ are solutions of this system, then $[y] = [z]$. It can be easily shown that if $y \in R$ is a solution of the system (3.4), then $[y]$ is an idempotent of the ring $R_{\mathfrak{I}}$. Thus we have proved:

THEOREM 3.2. *There exists a one-to-one correspondence between unitary divisors of the ideal $\mathfrak{I}$ and idempotents of the residue class ring $R_{\mathfrak{I}}$. More precisely, every idempotent in $R_{\mathfrak{I}}$ is a solution of the congruence system* (3.4), *where $\mathfrak{D}$ is a unitary divisor of the ideal $\mathfrak{I}$.*

If an idempotent $[f] \in R_{\mathfrak{I}}$ solves the system (3.4), where the ideal $\mathfrak{D}$ is a unitary divisor of the ideal $\mathfrak{I}$, then we again say that $[f]$ is the *idempotent belonging to the* (*unitary*) *divisor* $\mathfrak{D}$.

This implies, among others things, that we again have 2^r idempotents in the ring $R_{\mathfrak{I}}$. Similarly, primitive idempotent $[e_i]$, for every $i = 1, ..., r$, is the idempotent belonging to the unitary divisor

$$\mathfrak{I}_i = \frac{\mathfrak{I}}{\mathfrak{P}_i^{u_i}} = \prod_{\substack{j=1 \\ j \neq i}}^{r} \mathfrak{P}_j^{u_j}.$$

We leave for the reader the proof of the next result analogous to Lemma 2.2:

LEMMA 3.5. *Let $[e]$ and $[f]$ be two idempotents of the ring $R_{\mathfrak{I}}$ belonging to the unitary divisors $\mathfrak{T}$ and $\mathfrak{S}$ of $\mathfrak{I}$. Then*

(i) $I_{[e]} = J_{\mathfrak{I}/\mathfrak{T}}$

(ii) $[e] \wedge [f]$ *is the idempotent belonging to the unitary divisor* $\mathfrak{D} = \text{l.c.m.}(\mathfrak{T}, \mathfrak{S})$ *and* $J_{\mathfrak{D}} = J_{\mathfrak{T}} \cup J_{\mathfrak{S}}$.

(iii) $[e] \vee [f]$ *is the idempotent belonging to the unitary divisor* $\mathfrak{D} = (\mathfrak{T}, \mathfrak{S})$ *and* $J_{\mathfrak{D}} = J_{\mathfrak{T}} \cap J_{\mathfrak{S}}$.

(iv) $[e]'$ *is the idempotent belonging to the unitary divisor* $\mathfrak{D} = \mathfrak{I}/\mathfrak{T}$ *and* $J_{\mathfrak{D}} = \{1, ..., r\} \setminus J_{\mathfrak{T}}$.

The analogue of Theorem 2.3 is:

THEOREM 3.3. *If* $[f] \in R_{\mathfrak{I}}$ *is the idempotent belonging to the unitary divisor* $\mathfrak{D}$ *of* $\mathfrak{I}$, *then*

$$P^{R_{\mathfrak{I}}}([f]) = \bigcup_{\substack{\mathfrak{T} \mid \mathfrak{D} \\ \langle \mathfrak{T} \rangle = \mathfrak{D}}} [\mathfrak{T}]_{\sim}. \tag{3.5}$$

Proof. Let $[x] \in P^{R_{\mathfrak{I}}}([f])$ and let $[x]$ belong to the divisor $\mathfrak{T}$. Then $[x]^t = [f]$ for some $t > 0$, consequently, $[x]^t$ belongs to the divisor $((x^t), \mathfrak{I}) = ((x)^t, \mathfrak{I}) = \mathfrak{D}$. Thus a prime ideal $\mathfrak{P} \mid \mathfrak{T}$ if and only if $\mathfrak{P} \mid \mathfrak{D}$, i.e., $\mathfrak{T} \mid \mathfrak{D}$ and $\langle \mathfrak{T} \rangle = \mathfrak{D}$.

On the other hand, let $[x] \in R_{\mathfrak{I}}$ belong to a divisor $\mathfrak{T}$, where $\mathfrak{T} \mid \mathfrak{D}$ and $\langle \mathfrak{T} \rangle = \mathfrak{D}$. Then there exists a $t > 0$ such that $((x)^d, \mathfrak{I}) = \mathfrak{D}$ for every $d \geqslant t$. This implies that $[x]$ belongs to the idempotent $[f]$, i.e., $[x] \in P^{R_{\mathfrak{I}}}([f])$. ∎

The next two theorems are completely analogical to Theorems 2.5 and 2.6 of Section 2.

THEOREM 3.4. *Let* $[x] \in R_{\mathfrak{I}}$ *belong to a divisor* $\mathfrak{T} = \prod_{j \in J_{\mathfrak{T}}} \mathfrak{P}_j^{v_j}$, *where* $1 \leqslant v_j \leqslant u_j$ *for every* $j \in J_{\mathfrak{T}}$. *Then*

$$v([x]) = \begin{cases} 1 & \text{if} \quad \mathfrak{T} = 1 \ (J_{\mathfrak{T}} = \varnothing) \\ \max_{j \in J_{\mathfrak{T}}} \lceil u_j / v_j \rceil & \text{otherwise.} \end{cases} \tag{3.6}$$

This theorem in turn implies that

$$v^{(i)} = u_i.$$

If $[f]$ is the idempotent belonging to the divisor $\mathfrak{D}$ of $\mathfrak{I}$, then

$$v_{[f]} = \max_{j \in J_{\mathfrak{D}}} u_j = \mathscr{H}^R(\mathfrak{D}); \tag{3.7}$$

in the case $[f] = [0]$ we get

$$v_{[0]} = \max_{j \in \{1, \ldots, r\}} u_j = v_{R_{\mathfrak{I}}} = \mathscr{H}^R(\mathfrak{I}). \tag{3.8}$$

THEOREM 3.5. *Let* $[f]$ *be the idempotent of the ring* $R_{\mathfrak{I}}$ *belonging to the unitary divisor* $\mathfrak{D}$ *of* $\mathfrak{I}$. *Then*

(i) *The element* $[x]^{\mathscr{H}^R(\mathfrak{D})}$ *belongs to* $G^{R_{\mathfrak{I}}}([f])$ *for every* $[x] \in P^{R_{\mathfrak{I}}}([f])$.

(ii) *The element* $[x]^{\mathscr{H}^R(\mathfrak{I})}$ *belongs to a group for every* $[x] \in R_{\mathfrak{I}}$.

The numbers $\mathscr{H}^R(\mathfrak{D})$ *and* $\mathscr{H}^R(\mathfrak{I})$ *are the least positive integers possessing these properties.*

Theorem 2.7 can also be generalized for Dedekind rings:

THEOREM 3.6. *Let $[f] \in R_{\mathfrak{I}}$ be the idempotent belonging to the unitary divisor $\mathfrak{D}$ of $\mathfrak{I}$. Then the finite commutative rings $R_{\mathfrak{I}/\mathfrak{D}}$ and $[f]_{\mathfrak{I}} R_{\mathfrak{I}}$ with identities $[1]_{\mathfrak{I}/\mathfrak{D}}$ and $[f]_{\mathfrak{I}}$ are isomorphic.*

COROLLARY 1. *Let $[f] \in R_{\mathfrak{I}}$ be the idempotent belonging to the unitary divisor $\mathfrak{D}$ of $\mathfrak{I}$. Then the unit groups $G^{R_{\mathfrak{I}/\mathfrak{D}}}([1]_{\mathfrak{I}/\mathfrak{D}})$ and $G^{[f]_{\mathfrak{I}} R_{\mathfrak{I}}}([f]_{\mathfrak{I}})$ are isomorphic.*

Theorem 1.4 implies:

COROLLARY 2. *If $[e_i]$, $i = 1, ..., r$, are primitive idempotents of $R_{\mathfrak{I}}$, then*

$$G^{R_{\mathfrak{I}}}([e_i]_{\mathfrak{I}}) \simeq G^{R_{\mathfrak{P}_i^{u_i}}}([1]_{\mathfrak{P}_i^{u_i}}).$$

And again as at the end of Section 2.1 we see that for the determination of the values $\mu^{(i)}$, $\mu_{[f]}$, and $\mu_{R_{\mathfrak{I}}} = \mu_{[1]}$ the information about the structure of the groups $G^{R_{\mathfrak{P}^u}}([1]_{\mathfrak{P}^u})$, where $\mathfrak{P}$ is the prime ideal of the ring R and $u > 0$, is necessary.

3.2. *Prime Ideals in Field Extensions*

Other fundamental property of Dedekind rings says:

LEMMA 3.6. *Let R be a Dedekind ring of characteristic 0 and K its field of fractions. Let L be an extension of finite degree of K and S the integral closure of R in L. Then S is a Dedekind ring and an R-module of finite type.*

Let $\mathfrak{p}$ be a non-zero prime ideal of R. Then $\mathfrak{p}S$ is an ideal of S and it has here a factorization

$$\mathfrak{p}S = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}, \tag{3.9}$$

where $e_i > 0$, $i = 1, ..., r$. The ideals $\mathfrak{P}_i$ are just those prime ideals of the ring S for which $\mathfrak{P}_i \supset \mathfrak{p}S$. The exponent e_i $(i = 1, ..., r)$ is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Residue class rings $S/\mathfrak{P}_i$ and $R/\mathfrak{p}$ are in fact fields (Lemma 3.1 prime ideals $\mathfrak{P}_i$, $\mathfrak{p}$ are maximal) and $S/\mathfrak{P}_i$ can be regarded as finite dimensional vector space over $R/\mathfrak{p}$. The dimension f_i is called the *residual degree* of $\mathfrak{P}_i$ over R, $i = 1, ..., r$.

LEMMA 3.7. *With the preceding notations we have*

$$\sum_{i=1}^{r} e_i f_i = [S/\mathfrak{p}S : R/\mathfrak{p}] = n.$$

In the case of algebraic number fields as finite extensions of $\mathbb{Q}$, in the field of rational numbers we can take $R=\mathbb{Z}$ and $K=\mathbb{Q}$ and apply the previous results.

If L is a finite extension of $\mathbb{Q}$, then $L=\mathbb{Q}(\alpha)$, where (the so-called *primitive element*) $\alpha\in L$. We shall use the abbreviation $S=S^{\mathbb{Q}(\alpha)}$ for the ring of integers of the field $\mathbb{Q}(\alpha)$. This ring is Dedekind and satisfies the condition (FN).

Note that if $\mathfrak{P}$ is a prime ideal of S containing the ideal (p), with rational prime p and f the residual degree of $\mathfrak{P}$ over $\mathbb{Z}$, then $N(\mathfrak{P})=p^f$ (see e.g. [Nar1974]).

3.3. *Quadratic Fields*

Let $L=\mathbb{Q}(\sqrt{m})$, where m is a squarefree rational integer be a quadratic number field. Then

$$S=S^{\mathbb{Q}(\sqrt{m})}=\{a+b\omega;\, a, b\in\mathbb{Z}\},$$

where $\omega=\sqrt{m}$, if $m\equiv 2, 3 \pmod 4$ or $\omega=(1+\sqrt{m})/2$, if $m\equiv 1 \pmod 4$.

Let $\mathfrak{P}$ be a prime ideal of the ring S containing the ideal $(p)=pS$, where p is a rational prime. Let e and f be the ramification index and residual degree, respectively, of the prime ideal $\mathfrak{P}$. Then Lemma 3.7 shows that three cases are possible:

(i) $e=2$, $f=1$, then $\mathfrak{P}^2=(p)$ and we express this situation by saying that the prime ideal $\mathfrak{P}$ is *ambiguous of the first degree*. In this case the norm of the ideal $\mathfrak{P}$ is p, and the prime p ramifies in S.

(ii) $e=1, f=1$, then there exists a prime ideal $\mathfrak{Q}\neq\mathfrak{P}$ with $\mathfrak{P}\mathfrak{Q}=(p)$. We say that the prime ideal $\mathfrak{P}$ is *unambiguous of the first degree*. In this case the norm of the ideal $\mathfrak{P}$ is p, and the prime p splits in S.

(iii) $e=1, f=2$, then $\mathfrak{P}=(p)$. We say that the prime ideal $\mathfrak{P}$ is of the *second degree*. In this case the norm of $\mathfrak{P}$ is p^2, and the prime p remains prime in S.

The next theorem characterizes the prime ideals of S:

THEOREM 3.7. *Let $L=\mathbb{Q}(\sqrt{m})$ be a quadratic field, where $m\in\mathbb{Z}$ is squarefree. Let $\mathfrak{P}$ be a prime ideal of S containing the ideal (p), where $p\in\mathbb{Z}$ is a prime. Then*

(i) *The prime ideal $\mathfrak{P}$ is ambiguous of the first degree if and only if $p>2$ and $p\mid m$ or $p=2$ and $m\equiv 2, 3 \pmod 4$.*

(ii) *The prime ideal $\mathfrak{P}$ is unambiguous of the first degree if and only if $p>2$ and m is the quadratic residue modulo p or $p=2$ and $m\equiv 1 \pmod 8$.*

(iii) *The prime ideal $\mathfrak{P}$ is of the second degree if and only if $p>2$ and m is a quadratic non-residue modulo p or $p=2$ and $m\equiv 5 \pmod 8$.*

The complete characterization of the unit groups $G^{S_{\mathfrak{P}^u}}([1]_{\mathfrak{P}^u})$ of the ring $S_{\mathfrak{P}^u}$, where $\mathfrak{P}$ is a prime ideal of S, $u>0$, is given in [Ran1910] or [HaK1972]:

THEOREM 3.8. *Let $\mathfrak{P}$ be a prime ideal of the ring S containing the ideal (p), where p is a rational prime. Then*

(i) *If the prime ideal $\mathfrak{P}$ is ambiguous of the first degree, then*

(a) *for $p>2$,*

$$G^{S_{\mathfrak{P}^u}}([1]) \simeq \begin{cases} \mathbb{Z}_{p-1}\times\mathbb{Z}_{p^v}\times\mathbb{Z}_{p^{w-1}} \\ \qquad \text{if} \quad p>3,\ p\mid m \text{ or } p=3,\ m\equiv 3 \pmod 9, \\ \mathbb{Z}_2 \\ \qquad \text{if} \quad p=3,\ m\equiv -3 \pmod 9,\ u=1, \\ \mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_{3^{v-1}}\times\mathbb{Z}_{3^{w-1}} \\ \qquad \text{if} \quad p=3,\ m\equiv -3 \pmod 9,\ u>1; \end{cases}$$

(b) *for $p=2$,*

$$G^{S_{\mathfrak{P}^u}}([1]) \simeq \begin{cases} \mathbb{Z}_1 & \text{if} \quad m\equiv 2,\ 3 \pmod 4,\ u=1, \\ \mathbb{Z}_2 & \text{if} \quad m\equiv 2 \pmod 4,\ u=2, \\ \mathbb{Z}_4 & \text{if} \quad m\equiv 2 \pmod 4,\ u=3, \\ \mathbb{Z}_2\times\mathbb{Z}_{2^v}\times\mathbb{Z}_{2^{w-2}} & \text{if} \quad m\equiv 2 \pmod 4,\ u\geqslant 4, \\ \mathbb{Z}_{2^{v-1}}\times\mathbb{Z}_{2^w} & \text{if} \quad m\equiv 3 \pmod 8,\ u=2,\ 3,\ 4, \\ \mathbb{Z}_2\times\mathbb{Z}_{2^{v-1}}\times\mathbb{Z}_{2^{w-1}} & \text{if} \quad m\equiv 3 \pmod 8,\ u>4, \\ \mathbb{Z}_2 & \text{if} \quad m\equiv 7 \pmod 8,\ u=2, \\ \mathbb{Z}_4\times\mathbb{Z}_{2^{v-1}}\times\mathbb{Z}_{2^{w-2}} & \text{if} \quad m\equiv 7 \pmod 8,\ u>2, \end{cases}$$

where $v=\lfloor u/2\rfloor$, $w=\lfloor (u+1)/2\rfloor$ (here $\lfloor w\rfloor$ is the lower integer part of w, i.e., the largest rational integer z with $z\leqslant w$).

(ii) *If the prime ideal $\mathfrak{P}$ is unambiguous of the first degree, then*

$$G^{S_{\mathfrak{P}^u}}([1]) \simeq \begin{cases} \mathbb{Z}_{p-1}\times\mathbb{Z}_{p^{u-1}} & \text{if} \quad p>2,\ m \text{ is a quadratic} \\ & \qquad \text{residue modulo } p, \\ \mathbb{Z}_1 & \text{if} \quad p=2,\ m\equiv 1 \pmod 8,\ u=1, \\ \mathbb{Z}_2 & \text{if} \quad p=2,\ m\equiv 1 \pmod 8,\ u=2, \\ \mathbb{Z}_2\times\mathbb{Z}_{2^{u-2}} & \text{if} \quad p=2,\ m\equiv 1 \pmod 8,\ u>2. \end{cases}$$

(iii) *If the prime ideal* $\mathfrak{P}$ *is of the second degree, then*

$$G^{S_{\mathfrak{P}^u}}([1]) \simeq \begin{cases} \mathbb{Z}_{p^2-1} \times \mathbb{Z}_{p^{u-1}} \times \mathbb{Z}_{p^{u-1}} & \text{if } p>2, m \text{ is a quadratic non-residue modulo } p, \\ \mathbb{Z}_3 & \text{if } p=2, m \equiv 5 \pmod 8, u=1, \\ \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{2^{u-2}} \times \mathbb{Z}_{2^{u-1}} & \text{if } p=2, m \equiv 5 \pmod 8, u>1. \end{cases}$$

Let (3.1) be factorization of a proper ideal $\mathfrak{I}$ of the ring S with $\mathfrak{P}_i$ distinct prime ideals and $u_i>0$, $i=1, ..., r$. Then the previous theorem implies the required values of $\mu^{(i)}$ $(i=1, ..., r)$.

THEOREM 3.9. *Let* $\mathfrak{P}_i$ *be a prime ideal containing the ideal* $(p_i)=p_iS$, *where* $p_i \in \mathbb{Z}$ *is a rational prime. Then*

(i) *If the prime ideal* $\mathfrak{P}_i$ *is ambiguous of the first degree, then*

(a) *for* $p_i>2$

$$\mu^{(i)} = \begin{cases} (p_i-1)\, p_i^{v_i} & \text{if } p_i>3, p_i \mid m \text{ or } p_i=3, m \equiv 3 \pmod 9, \\ 2 & \text{if } p_i=3, m \equiv -3 \pmod 9, u_i=1, \\ 6 & \text{if } p_i=3, m \equiv -3 \pmod 9, u_i=2, \\ 2 \cdot 3^{w_i-1} & \text{if } p_i=3, m \equiv -3 \pmod 9, u_i>2; \end{cases}$$

(b) *for* $p_i=2$

$$\mu^{(i)} = \begin{cases} 1 & \text{if } m \equiv 2, 3 \pmod 4, u_i=1, \\ 2 & \text{if } m \equiv 2 \pmod 4, u_i=2, \\ 4 & \text{if } m \equiv 2 \pmod 4, u_i=3, \\ 2^{v_i} & \text{if } m \equiv 2 \pmod 4, u_i>3, \\ 2 & \text{if } m \equiv 3 \pmod 4, u_i=2, \\ 4 & \text{if } m \equiv 3 \pmod 4, u_i=3, 4, 5, \\ 2^{w_i-1} & \text{if } m \equiv 3 \pmod 8, u_i>5, \\ 2^{v_i-1} & \text{if } m \equiv 7 \pmod 8, u_i>5, \end{cases}$$

where $v_i=\lfloor u_i/2 \rfloor$, $w_i=\lfloor (u_i+1)/2 \rfloor$.

(ii) *If the prime ideal* $\mathfrak{P}_i$ *is unambiguous of the first degree, then*

$$\mu^{(i)} = \begin{cases} (p_i-1)\, p_i^{u_i-1} & \text{if } p_i>2, m \text{ is a quadratic residue modulo } p_i, \\ 1 & \text{if } p_i=2, m \equiv 1 \pmod 8, u_i=1, \\ 2 & \text{if } p_i=2, m \equiv 1 \pmod 8, u_i=2, \\ 2^{u_i-2} & \text{if } p_i=2, m \equiv 1 \pmod 8, u_i>2. \end{cases}$$

(iii) *If the prime ideal $\mathfrak{P}_i$ is of the second degree, then*

$$\mu^{(i)} = \begin{cases} (p_i^2 - 1)\, p_i^{u_i - 1} & \text{if } p_i > 2, \text{ } m \text{ is a quadratic non-residue modulo } p_i, \\ 3 \cdot 2^{u_i - 1} & \text{if } p_i = 2, \text{ } m \equiv 5 \pmod 8. \end{cases}$$

Let $[\varepsilon] \in S_{\mathfrak{I}}$ be the idempotent belonging to the divisor $\mathfrak{D}$ of $\mathfrak{I}$. Then Theorem 3.9 and relations (1.21) and (1.22) yield

$$\begin{aligned} \mu_{[\varepsilon]} &= \text{l.c.m.}\{\mu^{(j)};\, j \in J_{\mathfrak{I}/\mathfrak{D}}\}, \\ \mu_{S_{\mathfrak{I}}} &= \mu_{[1]} = \text{l.c.m.}\{\mu^{(j)};\, j \in \{1, \ldots, r\}\} \end{aligned} \tag{3.10}$$

and the generalized Fermat–Euler theorem for residue class ring $S_{\mathfrak{I}}$ of quadratic number field becomes the form:

THEOREM 3.10. *Let $[\varepsilon]$ be the idempotent of the ring $S_{\mathfrak{I}}$ belonging to the unitary divisor $\mathfrak{D}$ of $\mathfrak{I}$. Then*

$$\begin{aligned} [x]^{\mathscr{H}^S(\mathfrak{D}) + \mu_{[\varepsilon]}} &= [x]^{\mathscr{H}^S(\mathfrak{D})} \qquad \text{for every} \quad [x] \in P^{S_{\mathfrak{I}}}([\varepsilon]), \\ [x]^{\mathscr{H}^S(\mathfrak{I}) + \mu_{[1]}} &= [x]^{\mathscr{H}^S(\mathfrak{I})} \qquad \text{for every} \quad [x] \in S_{\mathfrak{I}}, \end{aligned}$$

where the numbers $\mu_{[\varepsilon]}$, $\mu_{[1]}$ are defined by (3.10). *Moreover, the numbers $\mathscr{H}^S(\mathfrak{D})$, $\mathscr{H}^S(\mathfrak{I})$ and $\mu_{[\varepsilon]}$, $\mu_{[1]}$ are the least positive integers for which these identities hold.*

Note that Theorem 2.13 is a special case of Theorem 3.10 with $m = -1$.

4. NUMBER FIELDS

Let $L = \mathbb{Q}(\alpha)$ be a number field of degree n and $S = S^{\mathbb{Q}(\alpha)}$ the ring of algebraic integers of L. Let $\mathfrak{P}$ be a prime ideal of S containing the ideal $(p) = pS$ with $p \in \mathbb{Z}$ a rational prime, i.e., $\mathfrak{P}$ appears in the factorization of the ideal (p) into a product of prime ideals. If e is the ramification index of the prime ideal $\mathfrak{P}$ over (p) and f is the residual degree of $\mathfrak{P}$ over $\mathbb{Z}$, then according to [Nak1979] we have for every $u > 0$:

$$G^{S_{\mathfrak{P}^u}}([1]) \simeq \mathbb{Z}_{p^f - 1} \times \prod_{t=1}^{\infty} \underbrace{\mathbb{Z}_{p^t} \times \cdots \times \mathbb{Z}_{p^t}}_{b_u(t)}, \tag{4.11}$$

where the coefficients $b_u(t)$ are also determined in the paper [Nak1979].

Let (3.1) be the factorization of the proper ideal $\mathfrak{I}$ of the ring S. Let the prime ideal $\mathfrak{P}_i$ contain the ideal (p_i), where $p_i \in \mathbb{Z}$ is a rational prime, and

let f_i be the residual degree of $\mathfrak{P}_i$ over (p_i) for $i=1, ..., r$. Then (4.11) implies the next result:

THEOREM 4.1. *If t_i is the largest positive integer with $b_{u_i}(t_i)>0$, then*

$$\mu^{(i)}=(p_i^{f_i}-1)\,p_i^{t_i}.$$

The order of the unit group $G^{S_{\mathfrak{P}_i^{u_i}}}([1])$ is [Nar1974]

$$\mathcal{N}(\mathfrak{P}_i)^{u_i-1}\,(\mathcal{N}(\mathfrak{P}_i)-1)=p_i^{f_i(u_i-1)}(p_i^{f_i}-1).$$

Since the exponent of a group is a divisor of its order,

$$t_i\leqslant f_i(u_i-1).$$

Let $[\varepsilon]\in S_{\mathfrak{I}}$ be the idempotent belonging to the divisor $\mathfrak{D}$ of the ideal $\mathfrak{I}$. Then Theorem 4.1 and relations (1.21), (1.22) give

$$\begin{aligned}\mu_{[\varepsilon]}&=\text{l.c.m.}\{\mu^{(j)};\ j\in J_{\mathfrak{I}/\mathfrak{D}}\},\\ \mu_{S_{\mathfrak{I}}}=\mu_{[1]}&=\text{l.c.m.}\{\mu^{(j)};\ j\in\{1, ..., r\}\}\end{aligned}\tag{4.12}$$

and the generalized Fermat–Euler theorem for residue class ring $S_{\mathfrak{I}}$ states:

THEOREM 4.2. *Let $[\varepsilon]$ be the idempotent of the ring $S_{\mathfrak{I}}$ belonging to the unitary divisor $\mathfrak{D}$ of $\mathfrak{I}$. Then*

$$[x]^{\mathscr{H}^S(\mathfrak{D})+\mu_{[\varepsilon]}}=[x]^{\mathscr{H}^S(\mathfrak{D})}\qquad \textit{for every}\quad [x]\in P^{S_{\mathfrak{I}}}([\varepsilon]),$$

$$[x]^{\mathscr{H}^S(\mathfrak{I})+\mu_{[1]}}=[x]^{\mathscr{H}^S(\mathfrak{I})}\qquad \textit{for every}\quad [x]\in S_{\mathfrak{I}},$$

where the numbers $\mu_{[\varepsilon]}$, $\mu_{[1]}$ are given by (4.12). *Moreover, the numbers $\mathscr{H}^S(\mathfrak{D})$, $\mathscr{H}^S(\mathfrak{I})$ and $\mu_{[\varepsilon]}$, $\mu_{[1]}$ are the least positive integers for which these identities are true.*

As the final application take a prime ideal $\mathfrak{P}$ of the ring S containing the ideal $(p)=pS$, where p is a rational prime. Let f be the residual degree of $\mathfrak{P}$ over (p). The unit group $G^{S_{\mathfrak{P}}}([1])$ of the residue class ring $S_{\mathfrak{P}}$ is cyclic and its order equals $\mathcal{N}(\mathfrak{P})-1=p^f-1$. Since $\mathscr{H}^S(\mathfrak{P})=1$ and the exponent of a cyclic group equals its order, we have

$$[x]^{p^f}=[x]$$

for every $[x]\in S_{\mathfrak{P}}$ what coincides with the Galois extension of the Fermat–Euler theorem mentioned in the introduction.

REFERENCES

[Bar1954] H. Barycz, Dzielo literacke Jana Brożka, *Pamiętnik Literacki* **45** (1954).
[Cro1983] J. T. Cross, The Euler Φ-function in the Gaussian integers, *Amer. Math. Monthly* **90** (1983), 518–528.
[Dic1919] L. E. Dickson, "History of the Theory of Numbers," Vol. I, Carnegie Institute, Washington D.C., 1919.
[FaM1958] H. K. Farahat and L. Mirsky, Group membership in rings of various types, *Math. Z.* **70** (1958), 321–244.
[HaK1972] F. Halter-Koch, Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern, *J. Number Theory*. **4** (1972), 70–77.
[Has1950] H. Hasse, "Vorlesungen über Zahlentheorie," Grundlehren der mathematischen Wissenschaften, Vol. 59, Springer-Verlag, Berlin/Göttingen/Heidelberg, 1950.
[Nak1979] N. Nakagoshi, The structure of the multiplicative group of residue classes modulo $\mathfrak{P}^{N+1}$, *Nagoya Math. J.* **73** (1979), 41–60.
[Nar1974] W. Narkiewicz, "Elementary and Analytic Theory of Algebraic Numbers," PWN, Warsaw, 1974.
[Ran1910] A. Ranum, The group of classes of congruent quadratic integers with respect to a composite ideal modulus, *Trans. Amer. Math. Soc.* **11** (1910), 172–198.
[Sie1959] W. Sierpiński, "Teoria Liczb," Vol. II, PWN, Warsaw, 1959.
[Sch1981] Š. Schwarz, The role of semigroups in the elementary theory of numbers, *Math. Slovaca* **31** (1981), 369–395.